Evaluating Claims about the Impact of RFID (Radio Frequency Identification) on Privacy and Security

Syed Qamar Raza, Chair/ Associate Professor, Mathematics and Computer Science Department, Talladega College, 627 West Battle Street, Talladega, AL 35160

Abstract

The proposed research project addresses the problem of representing and assessing claims about the effects of RFID technology on privacy and security. Sources will be scanned for claims about these effects, including contributions to assessing the claims and links to related claims. Clusters of claims will be formed and represented as part of an effort to provide useful information about the risks and safeguards for RFID deployment. The project will aim to emphasize the development of policy solutions as well as technological ones.

Problem Statement

Claims about the future impact of Radio frequency identification (RFID) on privacy vary in credibility, awareness and applicability. These claims include strong warnings about RFID threats to privacy and security as well as proposals for protecting privacy and security. The problem is the need to evaluate the threats and proposed counter-measures.

Introduction

Research Problem

In the context of pending societal issues and the urgent need to make decisions about deploying Radio Frequency IDentification (RFID) systems, major stakeholders in such a deployment need to be able to understand and assess the risks and protections associated with RFID systems. Both the technical and general literature concerning RFID effects on privacy appear to have tripled in amount from 2004 to 2005. Positions range from strong warnings against deploying RFID to reassurance that there is no problem in the deployment. The research problem is that of finding ways to represent and assess the claims about RFID threats to privacy and corresponding protections against threats.

Pending RFID Issues: There is much controversy about deploying Radio Frequency IDentification (RFID) systems, especially as a replacement for the Universal Product Code (UPC) system, currently accepted by both business and the general public, with
Electronic Product Code (EPC) based on RFID technology. Consider the following major issues.

Privacy versus security: In recent years, the public has had to deal with trading personal privacy for collective security, especially for entry into secure areas, such as terminals and buildings. Government actions, such as the USA PATRIOT act and the establishment of the Department of Homeland Security (DHS), have claimed the priority of securing accurate, integrated intelligence about individuals versus concern for individual privacy (Stone, 2004). The contents of one’s pockets and one’s identity are no longer sacred areas of privacy.

Costs versus benefits: Privacy advocates mainly see the costs of RFID. Business executives mainly see the benefits. Actually consumers and businesses have both costs (loss of both privacy and data security) and benefits (lower prices and efficiency).

Short term versus long term outlooks: Positions can differ as to whether the interest is in short term impacts of RFID deployment or in the long term effects. Immediate costs and benefits of a business decision might be in better focus than the long term trends. In contract, privacy advocates might focus on such decisions as setting precedents that put the society on a slippery slope towards a less free society.

Politics of personal information: Some sources treat personal information as if it were only a matter of protecting it as privacy (Perrin, 2005). But small businesses serving a small neighborhood of customers have been popular precisely because vendors know and use personal information to build trust and relationships. RFID tags triggering database information can enable the modern clerk to provide a similar warm, interested greeting. Personal information used properly is a tool used properly.

Persuasion versus education: The literature about RFID effects of privacy varies in the intention of the writer. Some write to persuade the reader; others to inform. Some use rhetoric and spin; others use facts and evidence.

Pending Decisions: It is too late to decide whether to start deploying RFID systems. They are already deployed throughout the world and probably exist in the lives of most every individual in the nation.

The extent and nature of deployment is still modifiable. Will it happen as a routine business decision with focus only on the bottom line, or will such decisions be constrained by professional standards and enlightened business principles?

The source or authority of regulation is also pending. Will the industry see the benefits of ethical self-regulation, as happens in many professions? Or will future uncontrolled development lead to lobbying-based governmental regulation? Given the heightened traffic on the Internet about RFID and Privacy, there is obviously an urgent need for an accurate assessment of claims about RFID and privacy.
Research Goals

1. Identify major RFID-Privacy claims (RPCs).
   The researcher will carefully mine the literature for specific claims about RFID effects on Privacy (RPCs). This effort will include identifying positions that address the same or similar claim, both supporting and discounting positions.

2. Develop instruments for representing and assessing RPCs.
   The research will develop at least the following instruments for representing and assessing claims about RFID effects on privacy:
   2.1 Descriptions of major claims, including rebuttals and summaries of relevant evidence and evaluations from multiple sources
   2.2 Graphic representations (networks) of relations among clusters of claims and counter-claims
   2.3 Summary verbal descriptions of identified RPC clusters
   2.4 A structured rating system for RPCs
   2.5 A risk assessment model for expected value of deciding whether to accept or reject specific RPCs

3. Perform validation and reliability measures on the above instruments.
   This includes comparing structured ratings of RPCs with less structured ratings of the same RPCs used by samples of stakeholders.

Questions

1. What are the claims made about effects of proposed RFID deployment on privacy?
2. How can such claims about threats and protections be related and evaluated?
3. Under what conditions are proposed privacy protections effective?
4. How might one evaluate the gains and losses of adopting particular strategies of using RFID and protecting privacy?

Literature support for significance of project:

Several ways demonstrate the significance of the research problem and the need for ways to represent and assess RPCs.

Historical scenarios: The World War II era created both the initial deployment of RFID as a friendly tool and reasons to be suspicious of personal identification and tracking. RFID technology produced what amounts to an electronic identification tag for returning bombers (Garfinkel, Jules & Pappu, 2005, p.34) Of course, plane identification already existed in terms of shape and markings, and the vocal challenge-password exchange was already a reliable technique for the foot soldier. But RFID was used to send an RF challenge to which the plane replied with a correct electronic ID signal.
People also became very afraid of governmental use of personal identification to do harm. Jews had a “J” on passports and patches on outer clothes to mark their ethnicity. The Germans also tattooed concentration camp inmates. (Gilbert, 1987, p. 469). In the U.S., records were used to identify Japanese Americans for collecting into internment camps. Such a type of scenario makes one cautious about guarding one’s identity and location. It is not hard to imagine an RFID tool being used as a weapon to do harm.

In the same era, George Orwell wrote 1984 (Orwell, 1950) and created the story of technology in which “Big Brother” knew who you were, where you were, and what you were doing; that is, a ubiquitous spying system. The fear of this scenario is possibly increased by current political moves to make intelligence and law enforcement agencies more capable of obtaining personal information.

Also in the same era and earlier, small businesses served small communities and were made more successful by a “Know your customer” strategy, being able to recognize customers by name and to know something about their personal lives. It was a good idea to ask the customer how the spouse and children were doing. It was a time when a waiter could anticipate what a steady customer would want. For some, RFID is a tool for providing such personal attention even in a large corporate world.

Major stakeholders: The literature also identifies the major stakeholders in the effects of RFID on privacy. Google.com searches show that the aggregate level of interest in RFID effects on privacy has risen dramatically. Civil Libertarians see their stake in protecting a right to privacy (Garfinkel & Rosenberg, 2005, p. 483). Consumers are concerned about privacy, but they would also respond favorably to reduced pricing due to RFID (Eckfeldt, 2005). Business people want to be more efficient in order to provide lower pricing, but they also need to be concerned with the security of data provided through RFID. Government people are expected to enforce civil liberties but also to stop crime by means of effective information gathering, possibly enhanced by RFID devices. Technology experts, such as research scientists and engineers, have a stake in understanding the effects and side effects of RFID (Heinrich, 2005; Juels, & Brainard, 2004). They may even take the position that it is not the technology itself that is the problem but the way the use of the technology is controlled (Stone, 2004).

Major positions: Concerning the deployment of RFID technology, the literature reveals three major positions:

- prevent deployment; avoid the slippery slope towards harmful effects on privacy (Albrecht, 2005), (Albrecht, and McIntyre, 2005), and (Givens, 2005)
- deploy RFID; it is beneficial to both customers and businesses and the privacy risks are not much (McGinity, 2004)
- delay deployment until effects on privacy are understood and countered by technology and social regulation (Givens, 2005)
Concerning the means of controlling RFID usage, the literature has two main approaches:
- develop technology to counter threats, a matter of making better devices
- develop policy to prevent threats, a matter of making better producers and users

Why the goal has not already been met:

Several sources have discussed in detail with balance and objectivity specific threats and remedies, including how serious is the threat and how effective would be the proposed (Ohkubo et al, 2005; Stone, 2004). But they appropriately either addressed in qualitative terms overall taxonomies of threats or in fairly technical terms specific characteristics of proposed solutions (Sanford, 2003; Windley, 2005; Weis el at 2003). There was no common yardstick by which to compare claims in such a way that the issue of deployment of RFID technology and privacy protection could be succinctly put and understood by the full range of stakeholders.

Some sources (Givens, 2005) already characterize the need to convince consumers, business executives and lawmakers that appropriate policy is needed. While many of the issues have to address specific levels of details, the general atmosphere surrounding deploying RFID needs to be understood by these parties. One needs to avoid attitudes inappropriately based on horror stories of abusive technology, oversimplification or one-sided views of issues, and public relations spins for short-term advantage.

Another factor is the tendency to polarize the issues in the tradition of favoring competition over cooperation as the means of succeeding. This research effort strives to make common representation and assessment more likely.

Feasibility of the Project

The level of technology needed to support this project is minimal. To collect data on how stakeholders evaluate claims and use the rating system will require some office supplies, postage, and perhaps some monetary incentives. The major effort will be the time needed to collect and process claims from a substantial body of literature.

Summary

Understanding and controlling the effects of RFID technology on privacy is complicated by the influences on the stakeholders. This project will develop means for fairly displaying a range of claims and interrelationships that determine decisions about deployment of RFID. This complex structure of ideas and influences concerns not only realistic privacy risks, but also the past, present and expected contexts that fuel stakeholder attitudes. It is very important that futurists consider not only the directions of technology development but also how human stakeholders are likely to react;
creating the need for policy to guide the professions, industries and societal members.

Review of Literature

In preparing this proposal, about a million technical references have been identified by Internet searches and more than 60 sources (Appendix D) have been read, primarily for identifying the claims about RFID privacy threats and proposed remedies.

Topics Found

Books have been written about RFID and Privacy (Albrecht & McIntyre, 2005; Garfinkel & Rosenberg, 2005; Heinrich, 2005). Some articles try to be objective about the controversy (Knapskog & Fiedler, 2004); Want, 2004; Weiss, 2003; Weiss et al, 2003). Most articles thus far reviewed for this project favor one side (RFID abuse of privacy) or the other (RFID usefulness). Articles emphasizing potential risks include (Albrecht, 2005; Garfinkel et al, 2005; Givens, 2005; Harper, 2004; Stajano, 2005). Stone (2004) makes the case that one should protest the abuse of technology rather than its development. Articles stressing the potential benefits include (Eckfeldt, 2005; Michael & McCathie, 2005; McGinity, 2005a). Molnar & Wagner (2004) describe technical and algorithmic protection in the context of library RFID tags.

Several sources propose privacy protection through technology, such as different types of tags for consumer protection (Heinrich, 2005; Juels et al, 2003) or legislation and regulation (Weinberg, 2005). Still others recommend better education of the consumer so that both and risks and benefits of EPC are understood (Givens, 2005; Hsi & Fait, 2005). This is especially true for those who fear privacy invasion but still want low prices.

What is problematic about replacing the UPC system with a RFID based EPC system? Consider these features:

1. UPC scanning requires line-of-sight, but RFID doesn’t. (Garfinkel & Holtzman, 2005). The current checkout scanners require that the barcode be visible to the scanner. Just as AM and FM radio waves pass through physical bodies, so too RFID radio waves pass through clothing and other means of blocking light. People are becoming familiar with similar capabilities of security scanners that can detect metal objects beyond the reaches of light.

2. Both readers and tags can be present without the knowledge of the consumer. The tag is millimeter size and one can deliberately hide it in an object. The readers also can be hidden or embedded in structures, such as “smart shelves” (Garfinkel et al, 2005)
3. Humans do not sense directly the scanning of a tag. In the UPC case one can observe the bar code passing by a reader. At this point in time there is little pressure to require notification or make a record of a RFID scan occurring.

4. Crucial to the issue of privacy is that RFID identification data has one more field than UPC: the item level serial number. This means that an object can be identified not only as to what type (model #) it is but also which unique object it is (serial #). This is essentially an electronic fingerprint. Expensive objects or dangerous ones commonly have serial numbers directly and plainly attached as signs for recall or anti-theft purposes. But with RFID, everything is uniquely labeled! If one has the habit of having the object on his person he is also as person uniquely identified, as surely as if he were recently hospitalized and still wearing a wrist tag.

5. Location of an individual can be monitored by RFID technology, either by a tag being combined with a GPS sensor (Curry, 2005) or by arranging for the tag to come in close proximity to a clandestine reader. The former has been deployed for monitoring children wandering in a theme park and for checking on the presence of students in school buses (Uzamere et al, 2005). An interesting example of the tag being in close proximity with a hidden reader is when a tag is embedded in the bottom of a shoe and the reader is hidden in a doormat (Albrecht, 2005).

6. RFID information can be collected and stored in databases for legitimate reasons but then, without the awareness of the consumer, the information is used for other purposes, like the selling of address lists. The IRS and Department of Homeland Security (DHS) would greatly benefit from unrestricted access to Social Security records. If a corporation included a credit card company, a medical insurance company, a major retailer, as well as book and videotape vendor, think of the connections and profiles that could be constructed on an individual, simply because his identity is known to each for legitimate reasons! UPC labels are not as universally useable.

**Sample Privacy Threats and Protections**

Some threats are unlikely to materialize.

Eavesdropping on the tag response (that sends its identification). Passive tags return a modulation of the energy in a radio wave from an authorized reader. The range of this tag response is only a few feet. This general means the spy reader is detectable because it is close to the tag, the shoe-doormat case described above being an exception. High cost self-powered tags have a large range but are too expensive to replace UPC labels.

It would be difficult to establish a secret network of readers such that they could report the location of a tag as it moves around. Cell towers inform a network that a phone is in the area, but those towers are hardly secret. On a small scale, as in the
monitoring a child in a park, an approved network could be established, but a “Big Brother” movement-tracking is not likely.

Some threats are present due to lack of regulation. It would be a straightforward matter to require all tags to beep when responding to a scan. But this is not being done. It would also be possible to build readers that would not interrogate tags that signaled a preference to be private. But this requires enforcement of a manufacturing standard for the readers (Garfinkel, 2002).

Some threats are real but with counteractions by technology. Spy sensors can eavesdrop on reader signals. If a reader sends a password to a tag, an unauthorized reader can detect it and therefore also send the password to the tag. There are technological ways to counter this.

- the tag could have a number of aliases that make spy readers fail to detect that an object moving from reader to reader is the same object. Of course, enough data collection from the tag could expose the set of aliases (Weis et al, 2003; Juels et al, 2003)

- the reader’s signal could be encrypted, although not in a sophisticated way by a low cost chip (Garfinkel, 2002)

- the relatively secure channel from tag to reader (a close low-energy transmission) could allow a secret random number to be a hash key know to both ends but unknown to eavesdroppers. The hashed identification will not be informative to the eavesdropper. (Garfinkel, 2002)

- blocker tags trick readers into thinking every possible serial number is nearby. For a 64 bit serial number, this ties up the reader with checking $2^{64}$ possible numbers. Such tags have a surround of electronic privacy; but since tools can become weapons, a blocker tag can also be used to sabotage normal reader service (Juels et al, 2003).

**Literature as Source of Claims to be Evaluated**

As a test of the ability to find claims in the literature, a sample of articles were search for the presence of specific claims. Unlike assessing a specific article containing a variety of claims; the focus of this task is to find a specific claim in a variety of different articles. Several chapters of Garfinkel & Rosenberg (2005) were in the sample, as well as a variety of articles from the Internet. Appendix A lists the results for just the preface of Garfinkel Rosenberg (2005).
Methodology

Major steps to goal

Claim collection. A claim would be a proposition presented as true. A sample claims list is found in Appendix A.

Claim analysis. There will be several ways in which claims will be processed.
    - Relevance to the effects of RFID on privacy. In other word, is the claim really related to RPC assessment? The concept of relevance remains to be operationalized. A structure for documenting contributions about claim and links to other claims is suggested in Appendix B

    - Clustering of claims. Clusters may be formed in a number of ways, such as opposing claims, claims about threat and remedies, claims clustered by stakeholder interest or type of RFID application.

    - Representing structure of RPC clusters. Within each cluster the claims relate to each other as suggested above. Relations such as supporting, opposing, implying are typical. Networks of nodes and edges can be used to represent such structure.

    - Global qualitative assessments. Most claims can be judged in overall ways, creating what amounts to considered opinions, often fueled by covert value assumptions. These would be available to compare with a rating system of simpler, more operationalized judgments.

    - Rating system. Such a system would require judgment of reasonably narrow features of a claim, such as its scope, depth, and the amount of evidence supporting it. A sample rating system is in Appendix C.

    - Stakeholder use of rating system. A stakeholder provides an internal context or attitude that shapes the rating judgments. Will this be a major factor? For example, will individual consumers rate in similar ways that differ from the ratings of technology experts?

Comparison of assessment instruments: The performance of various instruments will be compared. Reliability and validity measures will be estimated.

Expected value of decisions: Beyond assessing particular claims is the issue of which decisions to be made are the more consequential. The model being considered borrowed from signal detection theory (Heeger, 2003). Consider that a claim is either true or false and that the claim be either accepted or discounted. This involves four cases: true and accepted (a hit), true and discounted (a miss), false and accepted (a false alarm) and false and discounted (a reject). Probability estimates of two of independent cases will provide the expected value of a decision, which provides a measure of priority for making the decision.
Samples. Appendix C presents the results of testing the ease with which the rating system could be used on a variety of claims. This researcher found the system easy to use.

Methodological Issues

Focus on Claims. The core of the project is about relatively simple assertions (claims), not structured positions. Therefore, there is the possibility that information and significance is lost when the claim is taken out of context. Yet this is intentional. For example, is there any merit to the following claims:

- RFID tags can be read as far away as 30 feet (Albrecht, 2005)
- Reader networks for surveillance are feasible (Albrecht, 2005, chap 16)
- Killing the EPC tag at point of sale is necessary (Garfinkel & Rosenberg, 2005, Appendix B)
- Privacy is a social construct (Garfinkel & Rosenberg, 2005, Appendix B)
- Technologies are not neutral (Garfinkel & Rosenberg, 2005, Appendix B)

Qualitative versus Quantitative Measures: While some parts of the rating system will consider quantifiable features of a claim, the numerical ratings will ultimately be at best ordinal scales, such as below average, average, and above average. Moreover, like grading of student essays, there would a large amount of judgment involved. This does not mean, however, that the numerical ratings are not reliable. That would remain to be measured by standard methods.

Validity Testing: When ratings are found to be reliable, to what extent do they representations of the value or relevance a claim? It will be important to try the system across types of stakeholders and positions.

Summary

This approach will provide answers to the project’s research questions:
1. What are the claims made about effects of proposed RFID deployment on privacy?
2. How can such claims about threats and protections be related and evaluated?
3. Under what conditions are proposed privacy protections effective?
4. How might one evaluate the gains and losses of adopting particular strategies of using RFID and protecting privacy?

Of particular interest will be the results of representing how the claims and contributions to the claims, as well as relations among claims, allow one to have an accurate understanding of the effects RFID technology will have on privacy.
Appendixes

Appendix A
Sample Claims List

The following is a sample list of claims, taken entirely from the preface to Garfinkel & Rosenberg (2005).

1. RFID can be used for counterfeit prevention (authentication of drugs, documents)
2. RFID can be used to track people possessing tagged objects
3. RFID data collection from a single global network of readers is a threat to privacy.
4. RFID can be used to fight terrorism
5. RFID can be used to improve efficiency
6. RFID is vulnerable to industrial espionage
7. Any tool can also be a weapon
8. RFID enables keyless security
9. RFID enables object location
10. RFID leads to intrusive surveillance
11. Preserving privacy is costly
12. Option to participate in electronic toll collection reduces privacy
13. Both technology and policy solutions are needed.
14. RFID functions like a vehicle license plate
15. Almost any privacy threat by RFID can exist without using RFID
16. RFID experts need to educate public about RFID benefits
17. RFID effects need assessing before deployment
18. One has a right to know when one's tag is read

Appendix B
Structure for Claims Documentation

The following describes a format for organizing data for evaluating and linking claims. (*) indicates a repeatable segment.
(claim#)
Claim Statement
(Reference: identification of source
(Contribution to evaluating claim)*
)*
links: (claim#)*
)*
Appendix C
Rating System Variables

breadth (B)
    too narrow (1 – 3) too broad
depth (D)
    too shallow (1 – 3) too deep
#factors (F)
    few (1 - 3) many
#relations (R)
    few (1 – 3) many
evidence (E)
    weak (1 – 3) strong
analogies (A)
    weak (1 – 3) strong
type of argument (T)
    opinion oriented   (1)
    selected values    (2)
    fact oriented      (3)
Reference List


